Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015, The Internet Society, 2015.

[111] G. Agosta, A. Barenghi, G. Pelosi, and M. Scandale, "The MEET Approach: Securing Cryptographic Embedded Software Against Side Channel Attacks," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 34, no. 8, pp. 1320–1333, 2015.

[112] T. Jackson, B. Salamat, A. Homescu, K. Manivannan, G. Wagner, A. Gal, S. Brunthaler, C. Wimmer, and M. Franz, "Compiler-generated Software Diversity," in *Moving Target Defense - Creating Asymmetric Uncertainty for Cyber Threats*, vol. 54, pp. 77–98, 2011.

[113] A. Amarilli, S. Müller, D. Naccache, D. Page, P. Rauzy, and M. Tunstall, "Can Code Polymorphism Limit Information Leakage?," in *Proceedings of Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication - 5th IFIP WG 11.2 International Workshop, WISTP*, vol. 6633, pp. 1–21, 2011.

[114] A. Voulimeneas, D. Song, P. Larsen, M. Franz, and S. Volckaert, "dMVX: Secure and Efficient Multi-variant Execution in a Distributed Setting," in *EuroSec '21: Proceedings of the 14th European Workshop on Systems Security, Virtual Event / Edinburgh, Scotland, UK, April 26, 2021*, pp. 41–47, ACM, 2021.

[115] V. Le, C. Sun, and Z. Su, "Finding Deep Compiler Bugs via Guided Stochastic Program Mutation," in *Proceedings of the 2015 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications*, p. 386–399, 2015.

[116] R. Tsoupidi, R. C. Lozano, and B. Baudry, "Constraint-based Diversification of JOP Gadgets," *J. Artif. Intell. Res.*, vol. 72, pp. 1471–1505, 2021.

[117] J. Falleri, F. Morandat, X. Blanc, M. Martinez, and M. Monperrus, "Fine-grained and Accurate Source Code Differencing," in *ACM/IEEE International Conference on Automated Software Engineering, ASE '14*, pp. 313–324, 2014.

[118] H. Bostani and V. Moonsamy, "EvadeDroid: A Practical Evasion Attack on Machine Learning for Black-box Android Malware Detection," *CoRR*, vol. abs/2110.03301, 2021.

[119] D. D. Yao, X. Shu, L. Cheng, and S. J. Stolfo, *Anomaly Detection as a Service: Challenges, Advances, and Opportunities*. Synthesis Lectures on Information Security, Privacy, and Trust, Morgan & Claypool Publishers, 2017.

[120] S. A. Hofmeyr, S. Forrest, and A. Somayaji, "Intrusion Detection Using Sequences of System Calls," *J. Comput. Secur.*, vol. 6, no. 3, pp. 151–180, 1998.

[121] Y. Fang, C. Huang, L. Liu, and M. Xue, "Research on Malicious JavaScript Detection Technology Based on LSTM," *IEEE Access*, vol. 6, pp. 59118–59125, 2018.

[122] E. Johnson, D. Thien, Y. Alhessi, S. Narayan, F. Brown, S. Lerner, T. McMullen, S. Savage, and D. Stefan, ", : SFI safety for native-compiled Wasm," *Network and Distributed Systems Security (NDSS) Symposium*, 2021.

[123] F. Cohen, "Computer Viruses," in *Proceedings of the 7th DoD/NBS Computer Security Conference 1984*, pp. 240–263, 1986.

[124] R. L. Castro, C. Schmitt, and G. D. Rodosek, "ARMED: How Automatic Malware Modifications Can Evade Static Detection?," in *2019 5th International Conference on Information Management (ICIM)*, pp. 20–27, 2019.

[125] R. L. Castro, C. Schmitt, and G. Dreo, "AIMED: Evolving Malware with Genetic Programming to Evade Detection," in *18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 13th IEEE International Conference On Big Data Science And Engineering, TrustCom/BigDataSE 2019, Rotorua, New Zealand, August 5-8, 2019*, pp. 240–247, IEEE, 2019.

[126] W. Wang, Y. Zheng, X. Xing, Y. Kwon, X. Zhang, and P. Eugster, "WebRanz: Web Page Randomization for Better Advertisement Delivery and Web-Bot Prevention," FSE 2016, p. 205–216, 2016.

[127] H. Aghakhani, F. Gritti, F. Mecca, M. Lindorfer, S. Ortolani, D. Balzarotti, G. Vigna, and C. Kruegel, "When Malware is Packin' Heat; Limits of Machine Learning Classifiers Based on Static Analysis Features," in *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*, The Internet Society, 2020.

[128] M. W. J. Chua and V. Balachandran, "Effectiveness of Android Obfuscation on Evading Anti-malware," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, CODASPY*, pp. 143–145, 2018.

[129] P. Dasgupta and Z. Osman, "A Comparison of State-of-the-art Techniques for Generating Adversarial Malware Binaries," *CoRR*, vol. abs/2111.11487, 2021.